CH 8 IDENTITE DE BEZOUT

EX 31 :

1. Tout les entiers non nul et inférieurs à 7 sont premiers avec7donc $\varphi(7)=6$
   les entiers non nul , inférieurs à 8 et premiers avec 8 sont : 1 ;3 ;5 et 7
   donc $\varphi(8)=4$
2. Comme 0 n'est pas premier avec n ; alors il existe au plus n-1 entiers inférieurs à n et premiers avec n donc $\varphi(n)\leq n-1$
3. a/ p est premier donc tout les entiers non nul et inférieurs à p sont premiers avec p donc $\varphi(p)=p-1$
   b/ a non divisible par p et p premier alors d'après th de Fermat $a^{p-1}\equiv 1(p)$
   et comme $\varphi(p)=p-1$ alors $a^{\varphi(p)}\equiv 1(p)$
4. a/ p et q sont deux nombres premiers ;alors les nombres non premiers avec pq sont seulement les multiples de p ou les multiples de q
   Or il ya exactement q-1 multiples non nul de p inférieur à pq
   et il ya exactement p-1 multiples non nul de q inférieur à pq
   et il ya exactement pq-1 entier non nul et inférieur à pq
   Alors $\varphi(pq)= (pq-1) - [(q-1)+(p-1)]= pq-p-q+1=(p-1)(q-1)= \varphi(p).\varphi(q)$
   b/ On a $a^{\varphi(p)}\equiv 1(p)\Rightarrow (a^{\varphi(p)})^{\varphi(q)}\equiv 1(p)\Rightarrow a^{\varphi(p)\varphi(q)}\equiv 1(p)\Rightarrow a^{\varphi(pq)}\equiv 1(p)$
   On a $a^{\varphi(q)}\equiv 1(q)\Rightarrow (a^{\varphi(q)})^{\varphi(p)}\equiv 1(q)\Rightarrow a^{\varphi(q)\varphi(p)}\equiv 1(q)\Rightarrow a^{\varphi(pq)}\equiv 1(p)$
   Et comme $p\wedge q=1$
   Alors $a^{\varphi(pq)}\equiv 1(pq)$

Si($n\equiv 0(a)$; $n\equiv 0(b)$ et $a\wedge b=1$) Alors $n\equiv 0(ab)$

   c/ $1649=97\times 17$ (17 et 97 sont premiers ; $\varphi(17)=16$ $\varphi(97)=96$)
   10 n'est pas divisible par 17 et par 97 alors d'après b/
   $10^{16\times 96}\equiv 1(97\times 17)\Rightarrow 10^{1536}\equiv 1(1649)$
   $10403=101\times 103$ (101 et 103 sont premiers ; $\varphi(101)=100$ $\varphi(103)=102$)
   10430 n'est pas divisible par 101 et par 103 alors d'après b/
   $10430^{100\times 102}\equiv 1(101\times 103)\Rightarrow 10^{10200}\equiv 1(10403)$
5. a/ p étant premier donc seuls les multiples de p ne sont pas premiers avec p^k qui sont :1.p ;2.p ;3.p ;... ;$p^{k-1}.p=p^k$ Donc il ya $p^{k-1}-1$ entiers inférieur à p^k et non premiers avec p^k donc $\varphi(p^k)=(p^k-1)-(p^{k-1}-1)=p^k-p^{k-1}$
   b/ $\varphi(125)=\varphi(5^3)=5^3-5^2=100$;$\varphi(256)=\varphi(2^8)=2^8-2^7=128$; $\varphi(1331)=\varphi(11^3)=11^3-11^2$
6. a/ $(1+up)^{p^{k-1}}=\sum_{j=0}^{p^{k-1}} C_{p^{k-1}}^{j}(u.p)^j=1+\sum_{j=1}^{p^{k-1}} C_{p^{k-1}}^{j}(u.p)^j$

   et comme p^{k-1} *divise* $C_{p^{k-1}}^{j}$ *Alors* p^k *divise* $C_{p^{k-1}}^{j}(u.p)^j\ \forall j\in\{1;2;...;p^{k-1}\}$

   b/ (Par récurrence) * Pour k=1 La propriété est vrai d'après 3. b/
   *Soit $k\in IN^*$ supposons que $a^{\varphi(p^k)}\equiv 1(p^k)\Rightarrow a^{\varphi(p^k)}=1+u.p^k$
   Et montrons que $a^{\varphi(p^{k+1})}\equiv 1(p^{k+1})$
   D'après 5. a/ on a $\varphi(p^k)=p^k-p^{k-1}\Rightarrow \varphi(p^{k+1})=p.\varphi(p^k)$
   Donc $a^{\varphi(p^{k+1})}=a^{p.\varphi(p^k)}=(a^{\varphi(p^k)})^p=(1+u.p^k)^p\equiv 1(p^{k+1})$

Pour a=17 ;p=5 et k=3 on obtient $17^{100}\equiv 1(125)$; pour a=17 ; p=2 et k=8 on obtient...

Qarray.tn Adra Blech Qarray.tn